Cryptez, cryptez, mais en restera-t-il toujours quelque chose?

Dinant, Jean-Marc

Published in:
Actualités Juridiques Vie Privée, Transparence et Nouvelles Technologies

Publication date:
2002

Document Version
le PDF de l'éditeur

Cryptez, cryptez, mais en restera-t-il toujours quelque chose ?

Jean-Marc Dinant

Les défenseurs des libertés individuelles en général et de la vie privée en particuliers se sont émus dans le monde entier suite à l'adoption en catastrophe de lois censées éradiquer le terrorisme, par le sénat américain, suivi par les Anglais, les Canadiens et les Français[1]. En réaction à cette surveillance exploratoire et généralisée du réseau Internet, de nombreux citoyens n'ayant rien d'autre à cacher que leur vie privée se demandent, une fois de plus, si la cryptographie ne serait pas la solution simple et universelle pour garantir la confidentialité de leurs données sur Internet.

Echelon sur-estimé

Une question se pose alors face aux Echelon et autres système Carnivore : la cryptographie est-elle une garantie suffisante face aux pouvoirs inconnus des services secrets ? Les services secrets notamment américains ne posséderaient-t-ils pas les moyens de décrypter n'importe quel message chiffré.

Le rapport Poullet-Dinant[2] a démontré que les capacités du réseau Echelon sont énormes mais non connues avec certitude. Si le réseau d'interception Echelon existe bel et bien, ses capacités d'interception sont bien moindres que ce qui fut souvent imaginé par la presse. Notamment, la technologie de reconnaissance vocale n'est pas suffisamment au point actuellement pour permettre à un ordinateur de reconnaître des mots-clés dans un discours téléphonique.

Dans son rapport 2001, le Comité R s'est interrogé sur le danger présenter par la NSA-KEY, une clé de la base des registres des systèmes d'exploitation crée par Microsoft. D'aucuns ont prétendu que cette clé "secrète" (mais stockée en clair sur le disque dur de chaque PC Windows) permettrait à la NSA de déchiffrer n'importe quel message établi à l'aide des logiciels cryptographiques conçu par Microsoft. Citant un des auteurs du rapport évoqué supra, le Comité R en conclut avec justesse[3] que ces accusations sont très probablement non fondées. En fait il existe d'autres moyens bien plus discrets et plus efficaces pour décrypter un système. En outre le scénario évoqué supra supposerait des complicités sans faille à plusieurs niveaux de la société Microsoft, ce qui semble difficile même pour la NSA.

L'illustration en a été faite lors de la dernière affaire en date aux Etats-Unis dans le cadre de l'affaire Nicodemo Scarfo. Cette personne, soupçonnée de paris illégaux avait

1 *http://www.internet-actu.com/archives/une/une108.html*

2 *Poullet Yves, Dinant Jean-Marc, "Le réseau Echelon : Existe-t-il ? Que peut-il faire ? Peut-on et doit-on s'en protéger ?" Rapport d'expertise rédigé à l'attention du Comité Permanent de contrôle des services de renseignements. Mars 2000. Disponible sur* **http://www.droit.fundp.ac.be/textes/** *echelonfr.pdf*

3 *Rapport d'activités 2000 à l'attention du Comité Permanent de contrôle des services de renseignements, pp 52-54*

encrypté ses données à l'aide du programme PGP[4]. Le juge avait délivré un mandat de perquisition permettant aux enquêteurs de visiter le bureau de la personne soupçonnée. Le FBI a lors d'une de ces visites placé un système[5] de type "key logger system" KLS sur l'ordinateur du suspect. Ce KLS a pris note des touches enfoncées sur le clavier lorsque la machine étant non connectée au réseau via un modem et le FBI a pu ainsi connaître la valeur de la clé secrète utilisée. Récemment EPIC a mis en ligne la déposition d'un responsable du FBI qui a détaillé la méthode utilisée. Cet événement est rassurant. Il tente à prouver qu'un système comme PGP est inviolable en soi et que la seule manière de le vaincre est de le contourner en tentant de saisir la clé secrète d'encryptage/décryptage, au moment où elle est tapée sur le clavier.

Loin d'être efficaces contre le terrorisme, les nouvelles lois votées dans la précipitation et sous le coup d'une émotion bien légitime risquent de créer deux effets pervers déjà signalés dans le rapport Poullet-Dinant[6], effets pervers liés à l'existence du réseau Echelon mais qui, paradoxalement (?) trouvent à s'appliquer à ces lois "patriotiques":

1. *Il existe un risque d'apparition anarchique de solutions techniques de cryptage de plus en plus performantes, rendant difficile voire impossible l'interception légale du contenu des télécommunications."*

2. *Il existe un risque croissant du développement d'une réticence à l'utilisation des réseaux, notamment dans le cadre du commerce électronique, mais aussi dans le cadre de l'utilisation d'Internet à des fins non commerciales. Nous pensons par exemple à l'utilisation d'Internet pour la recherche d'informations politiques, médicales, religieuses, philosophiques, scientifiques ou culturelles et à la participation à des forums publics de discussion. Le sentiment d'être espionné, même en l'absence de tout fondement scientifique raisonnable, risque d'être un obstacle majeur au développement de l'utilisation des réseaux de télécommunication.*

Effets négatifs pour l'économie

Il est étonnant que Georges W(ar) Bush et son équipe ne s'inquiètent pas d'avantage des retombées nocives de ce type de loi pour l'économie américaine et la sûreté nationale. Il n'est jamais évident d'éviter la peste sans attraper le choléra. Gymnastique d'autant plus acrobatique qu' il ne s'agit pas seulement d'éviter la peste et le choléra mais bien aussi ce fameux anthrax qui n'a rien d'un hoax[7]. Il existe en effet un troisième risque attribué[8] au réseau Echelon *: l'écoute politique menée par des partis politiques au pouvoir ou des membres de ceux-ci afin d'espionner les adversaires politiques. On peut rappeler le scandale du Watergate ou les écoutes effectués par l'Elysée en France. Il reste extrêmement tentant pour un parti au pouvoir de surveiller ses adversaires démocratiques afin d'obtenir sur lui un avantage politique déterminant. Ce type d'écoute sape le jeu normal de la démocratie et tout état démocratique se doit de les empêcher.*

Avec une loi anti-terrorisme des données personnelles ?

4 *Inventé par Paul Zimmermann, ce système cryptographique est considéré encore comme aujourd'hui comme étant un des plus sûr au monde. Pour preuve, son auteur a été attaqué sur base de violation de la loi américaine interdisant l'exportation de programmes de cryptage sans l'aval de la NSA ("*NSA provides the Department of State with technical advice to determine whether the commodity is a cryptographic system, equipment, assembly, module, integrated circuit, component or software "with the capability of maintaining secrecy or confidentiality of information" *covered under Category XIII(b)(1) of the United States Munitions List ("USML"). 22 C.F.R. § 121.1, XIII(b)(1). Cfr http://people.qualcomm.com/karn/export/crowell.html, visité en août 2001. Toutefois la justice américaine a considéré que l'exportation d'un algorithme de chiffrement ou du code d'un programme informatique ne peut être considérée comme un système cryptographique mais relève de la liberté d'expression garantie par la Constitution américaine.*

5 *Selon l'aveu même du FBI, ce type de système peut être placé dans le hardware, le firmware ou le software. Où à plusieurs endroits simultanément.*

6 *op. cit. p.36*

7 *Intox en anglais. Les Hoax (fausses alertes vis-à-vis des virus inexistants) causent apparemment autant de troubles que les vrais virus en semant la panique en un temps record sur le réseau.*

8 *Cité en premier lieu par les mêmes auteurs. Op. cit. ibid.*